IDAHO CONSUMER NEWS

Volume 1, Issue 4 | **Office of Attorney General Lawrence Wasden** | **Summer 2006**

The Internet and Computer Safety Issue!

Attorney General Lawrence Wasden

Office of Attorney General
700 W. Jefferson Street
P.O. Box 83720
Boise, ID 83720
Phone (208) 334-2400
Fax (208) 334-2530

Consumer Protection
Civil Litigation Division
Phone (208) 334-2424
or Toll Free in Idaho at:
1-800-432-3545
Fax (208) 334-2830

In This Issue

Night of the Living Botnet

Computer Hackers Letting You do their Dirty Work

Do you hate SPAM e-mail ads? Did you know that your computer could be sending them without your knowledge? Yes, your computer may be a "zombie" slave, working to make money for criminals who control vast "botnet" armies. A hacker can turn your computer into a zombie by exploiting security weaknesses in its system, infecting it with a virus or Trojan horse program, and then gaining control of it by remote access. Once hackers have gained this access, they can do anything you can do on your computer.

A botnet is a network of zombie computers that are all controlled by a single hacker. A single botnet could contain hundreds of thousands, or even more than a million computers. The amount of capacity a hacker steals from each computer is small, too small to be noticed by the common owner. However, when multiplied by a million computers, the hacker controls a powerful network.

Recent estimates say zombie computers may be responsible for 50 % to 80 % of all spam..

Criminals have realized the profit potential of your computer. They make money using it to send e-mails advertising products, holding websites hostage to Denial of Service (DoS) attacks, spreading computer viruses that steal information, and committing "click fraud" against pay-per-click websites. Recent estimates suggest that zombie computers may be responsible for 50% to 80% of all spam.

Some criminals use botnets to hold websites for ransom. A business will receive a demand to pay a certain amount, often tens of thousands of dollars, to the criminal. The message includes a threat that, if the business doesn't pay, the business's website will be shut down by a DoS attack. In a DoS attack, the criminal orders all of the bots to contact the website at the same time, overloading the bandwidth and effectively shutting the site down.

You may find your messages blocked by anti-spam filters. Your Internet service provider may disconnect you if it gets complaints about your computer sending spam.

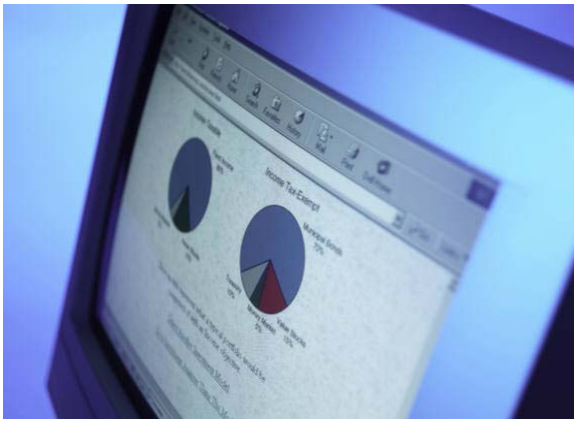
If your computer is connected to the Internet, and not protected by antivirus software, it could be compromised within five minutes. If your internet connection suddenly slows down, or the mouse or keyboard are unresponsive; if you get bounceback messages from people you have not emailed; or, if your hard drive seems hyperactive, your computer may be a zombie. You may find your messages blocked by anti-spam filters. Your Internet service provider may disconnect you if it gets complaints about your computer sending spam.

See Zombies on page 2

continued from page 1

Zombies

If you experience any of these problems, you may want to have a computer repair professional examine your system to see if it is a zombie.



To avoid a zombie takeover of your computer, make sure you have a reliable antivirus program and keep it updated. You also need a firewall. Some firewalls are sold with antivirus programs as part of Internet security packages. Firewalls are also sold separately. Keep your operating system and browser updated. Many hackers exploit holes or vulnerabilities in these programs. You can patch these vulnerabilities with updates from your software provider.

Never open attachments in e-mails unless you know and trust the person who sent them. You should also never download files from websites unless you are sure they're safe. Some hackers take advantage of file sharing networks rather than e-mails to spread their viruses. ❖

Spy Versus Anti-Spy

Your homepage has been changed. Searches are redirected to unwanted sites. Favorite folders are filled with unwanted entries. You discover unfamiliar toolbars. You experience many pop ups. Your computer runs slowly. Your firewall disappears. Is this a nightmare? No, it is spyware.

Spyware is software that has been loaded onto your computer without your knowledge or consent. There are two types of spyware:

- Advertising spyware: this type of spyware takes over your computer. Whoever is controlling it shows you advertisements by redirecting your searches.
- Surveillance spyware: this spyware can collect passwords, credit card and banking information, email addresses, social security numbers. It can be a first step in stealing your identity.

Spyware is typically added to a computer when you download free software from the Internet. In other cases, simply visiting web pages can add spyware to your computer.

To prevent spyware from invading your computer:

- Update your operating system and Web browser software. Set your browser security to detect unauthorized downloads.
- Use anti-virus and anti-spyware software, as well as a firewall. Update them regularly.
- Download free software only from sites that you know and trust.
- Do not click on links inside pop-up windows.
- Do not click on links from unknown email sources that claim to offer anti-spyware software. You could actually be installing spyware.

If you think that you are a victim of spyware:

- Get an anti-spyware program from a vendor that you know and trust.
- Set the anti-spyware program to scan on a regular basis – at least once a week – and every time you start your computer.
- Delete any software programs the anti-spyware program detects that you do not want on your computer.

If you discover spyware on your computer, file a complaint with the Federal Trade Commission at www.ftc.gov.

For more information on preventing and battling spyware go to www.ongaurdonline.gov/spyware.

VIRUSES

Have you ever tried to log on to your computer or open a program and it seems to take forever? It may not be that your computer is old or that it does not like you. It could be a virus.

A computer virus works in computers much like viruses work in people. The virus is a piece of code, or instructions, that tell the computer to make copies of the virus and spread it to other computers. Just as a flu epidemic can infect a human population, a computer virus can spread through a network by email attachments or files people download and share.

Many viruses are connected to other files. Music files and even screensavers could be viruses in disguise. Standard viruses are software which attaches to programs (like Word or Excel) and runs every time the program is run. Each time the virus gets a chance to run, it may multiply, harm, shut down, or do other detrimental things to your computer. Viruses can also come through email. These viruses are usually activated when the message is opened or when an attachment is opened. It can come from known sources or SPAM. It usually replicates itself by automatically sending messages from a victim's address book.

Other common viruses are Worms and Trojan Horses. Worms are viruses that, instead of using programs, use computer networks and security holes. Worms find the holes, replicate, and continue to scan for other holes to continue to replicate. A Trojan Horse is software you download with the belief that it is a legitimate program, such as a game or a pop-up blocker. When it is run, it may cause your computer to crash or completely erase the hard drive. A Trojan Horse does not replicate itself, however it can send a message back to the creator of the virus who can then gain access to your computer and turn it into a zombie.

Although viruses come in many shapes and forms, you can protect yourself by using anti-virus programs and keeping them updated. It is also good to use a firewall, which prevents hackers from getting into your system.

If you find your computer is infected, immediately disconnect from the Internet, scan with up to date anti-virus software, and report any unauthorized use of your computer to your Internet Service Provider.

Recent Consumer Protection Settlements

LUPRON: The State of Idaho entered into a settlement with manufacturer TAP Pharmaceutical Products, Inc. involving the prescription drug Lupron. Lupron has been used to treat prostate cancer, endometriosis and early puberty. The State will receive $198,000 from this settlement, and the money will be used to reimburse Idaho consumers who purchased the drug and did not file a claim in the national class action lawsuit. Refunds may be up to $100, or 50% of a consumer's out-of-pocket expenses, whichever is greater. The settlement addresses the pricing of the drug, not the safety of the drug.

YELLOW PAGES, INC.: Idaho consumers and businesses are entitled to refunds from YPI, a Nevada corporation, as a result of a legal settlement. The company (an independent publisher of regional business-to-business and Internet telephone directories) solicitations to Idaho consumers and small businesses. The settlement requires YPI and sister company Electronic Directories, LLC to provide refunds to Idaho consumers who cashed small checks and then paid for advertising they had no intention of purchasing.

Please contact the Consumer Protection Unit at (208) 334-2424 or (800) 432-3545 if you have any questions regarding either these or other settlements. ❖

Fair Time!

It is getting close to that time again. The fair and rodeo season is upon us and that means it is time for The Attorney General's Office to get out and meet you. This year we will be attending four fairs: the Western Idaho, Northern Idaho, Twin Falls County, and Eastern Idaho Fairs.

Our focus this year is the Attorney General's ProtecTeens program. The ProtecTeens video and resource kit were developed by the Attorney General and the Secretary of State. The program helps parents and teens avoid online sexual predators and navigate the Internet safely. We will have an educational booth at each fairwith ProtecTeens CDs for parents and teens.

We will also be prepared to answer your questions regarding other consumer topics, including Buying Used Vehicles, Landlord Tenant Issues, Lottery Scams, and much more.

Enjoy the summer. We hope to see you at the fair! ❖

Peer-To-Peer Peril

Many proficient PC users enjoy sharing the latest joke emails, chat sites, and downloads. You probably know people who enjoy sharing files of many different varieties. Maybe you share files yourself.

If you do, be wary. By downloading music, games, or software, you might unknowingly mire yourself in legal trouble, virus downloads, or identity theft.

Peer-to-peer file-sharing, or "P2P", occurs when files are shared from one computer to another on a network. P2P file-sharing is illegal when users share copyrighted materials without permission from the owner. Copyrighted materials include music, movie files, TV programs, books, and images.

By law, you are not allowed to have share any copyrighted material that you do not own. For instance, if you download a movie that you already own, it is probably legal, but if you download a movie that you did not own, it is probably illegal, unless you get permission from the owner. Distributing a file to another person, whether selling it or giving it, is also illegal, unless that person also owns the file or has permission from the owner.

Illegal file-sharers can face criminal penalties of up to 5 years in prison and $250,000 in fines. There are also civil penalties of up to $150,000 *per violation*. Every time you send a file, you violate the law another time!

Those that file-share may also be transmitting personal information inadvertently on the Internet. In addition to the potential for the file to conceal a virus, many file-sharing programs are bundled with "spyware" or "adware". These programs monitor your Internet activity and will relay any personal information to advertisers. The also drastically slow down the performance of your computer.

To combat risks associated with P2P file-sharing:

- Buy and update anti-virus programs.
- Buy software that can detect or prevent spyware downloading.
- Use the suggested settings from your software provider for file-sharing.
- Close your connection after completing the file-sharing.
- Do not share copyright files (unless you have expressed written consent from the copyright owner).

Tidbits

Computer Donation

Q: Is it possible to donate used computers?

A: Yes. If your computer is less than five years old, it may be a very good candidate for donation.

Q: To whom should I give?

A: Charities and schools are great places to donate old computers. However, it is best to donate them through a computer refurbisher to make sure that the hard drive is clean and the software is legal.

Q: What if my computer is older than five years and parts of it are broken?

A: If your computer is damaged or some of the equipment is not working properly, it is best to recycle it through a computer recycling business or organization.

Q: Do I need to worry about my personal information?

A: Yes, It is extremely important to make sure your computer is cleaned of all documents. It is a good idea to get disk cleaning software if you are going to clean your computer on your own. Disk cleaning software will help to completely erase your Internet history, emails, cookies, and various documents on your computer.

Q: Do I need to provide a refurbisher with anything other than the computer?

A: It is helpful if you provide the accessories (keyboard, mouse, modem, etc.). It is also extremely helpful if you provide the operating system intact, original media and documentation. Providing the original software materials will help to keep everything legal for the recipient of the donation.

❖